REMARKS

The Applicants have studied the Office Action dated March 11, 2005 and have made amendments to the claims to distinctly claim and particularly point out the subject matter which the Applicants regard as the invention. No new matter has been added. It is submitted that the application, as amended, is in condition for allowance. Claims 1, 3-9, 11-16, 18-20, and 22 have been amended. Claim 21 has been cancelled without prejudice or disclaimer. Claims 2, 10, and 17 were cancelled in a previous amendment. By virtue of this amendment, claims 1, 3-9, 11-16, 18-20, and 22 are pending. Reconsideration and allowance of the pending claims in view of the above amendments and the following remarks is respectfully requested.

In the Office Action, the Examiner:

(1-2) noted claims 1-16 are pending in the application, claims 2, 10, and 17 are cancelled, and claims 18-22 are added; and

(4) rejected claims 1, 3-9, 11-16, and 18-22 under 35 U.S.C. § 103(a) as being unpatentable over Stefik (U.S. Patent No. 5,715,403) in view of Yoshiura et al. (U.S. Patent No. 6,131,162), and in view of Johnson et al. (U.S. Patent No. 6,591,250).

Overview of the Present Invention

The present invention is directed to a method, system and computer readable medium for updating previously stored usage conditions to allow additional uses of previously received encrypted digital content to be performed. The present invention overcomes the time consuming problem of re-downloading content when an end user has a license for the content and desires to purchase another use of the content, which the end user has already previously downloaded. Stated differently, the present invention permits an end user to update usage conditions in lieu of re-downloading the digital rights management protected content.

(4) Rejection under 35 U.S.C. §103(a) over Stefik in view of Yoshiura et al. and in view of Johnson et al.

As noted above, the Examiner rejected claims 1, 3-9, 11-16, and 18-22 under 35 U.S.C. § 103(a) as being unpatentable over Stefik (U.S. Patent No. 5,715,403) in view of Yoshiura et al. (U.S. Patent No. 6,131,162), and in view of Johnson et al. (U.S. Patent No. 6,591,250).

Before discussing the prior art in detail, it is believed that a brief review of the invention as claimed, would be helpful. Amended independent claim 1 recites, *inter alia*:

> ...
> **receiving from an electronic store, a hash value**, which uniquely identifies the encrypted digital content, associated with the request to acquire the encrypted digital content;
> **comparing the hash value received from the electronic store with a previously stored hash value** corresponding to the previously received encrypted digital content;
> **updating the usage conditions** associated with the previously received encrypted digital content **in response to the hash value received matching the previously stored hash value**; and
> **permitting at least one additional use** of the previously received encrypted digital content **without the need to re-receive the received encrypted digital content.** (emphasis added)

During the initial creation of the encrypted digital content, a hash value is created. The hash value is basically a fingerprint of the message and uniquely identifies that particular digital content to the exclusion of others. Page 31, 3rd para. of the instant application.

When an end user makes a purchase, the hash value is placed in the Transaction SC(s) 640 that is sent to the End User Device(s) 105. A Helper Application 109 on the End User Device(s) 105 stores the hash value in the local license database 197 for the specific Content 113. Page 164 of the instant application.

When a second copy (or additional copy) of the identical Content 113 is purchased, a second copy of the hash value, identifying the previously transmitted digital content, is

received. Page 164 of the instant application. ("*receiving...a hash value, which uniquely identifies the encrypted digital content, associated with the request to acquire the encrypted digital content*". Claim 1 of the instant application.)

The Player Application 196 searches the local license database 197 for the digital content 113. *Id.* If the content 113 already exists in the local database 113, then a comparison is made of the hash from the new Transaction SC(s) received during the end users' request for a second copy of the digital content. *Id.* ("*comparing the hash value received with a previously stored hash value corresponding to the previously received encrypted digital content*". Claim 1 of the instant application.)

If hash values are identical, then usage values associated with the digital content 113, such as number of allowable copies, are updated ("*updating the usage conditions associated with the previously received encrypted digital content in response to the hash value received matching the previously stored hash value*" Claim 1 of the instant application.) and the end user can make additional copies. *Id.* ("*permitting at least one additional use of the previously received encrypted digital content without the need to re-receive the received encrypted digital content*" Claim 1 of the instant application.) In this way, another time-consuming download of the Content from the Content Hosting Site(s) 111 can be avoided because the Content 113 is exactly the same content as previously downloaded.

On the other hand, if the hash values are different, then the content requested must be downloaded from the Content Hosting Site(s) since something, i.e., the content itself, the artwork, or other metadata relevant to the Content 113, has changed. The advantage of this invention is that consumers who purchase an additional copy of content that they already have downloaded do not have to go through the tedious process of re-downloading that specific content again. Instead, the Usage Rights 519 associated with the content previously received is updated.

As the Examiner correctly states on page 4 of the above-identified Office action, "*Stefik does not disclose about comparing a stored hash value.*" The Examiner then goes on

to combine Yoshirua et al. and Johnson et al. with Stefik.[1] Both the Johnson et al. and the Yoshiura et al. references use hash values **only** for the purpose of verifying the authenticity of a message from a sender. In both references, a cryptographic hash value is dynamically computed for a file at the time of transmission. The file is then sent to a destination, along with the hash value. The receiver then **computes** a second hash value and compares it to the original hash value generated for the message to ensure that the file was not altered during transmission.[2] See Yoshiura at col.2, lines 11-19 and Johnson et al., col. 10, lines 14-17. Thus, both Johnson et al. and Yoshiura et al. specifically teach computing two hash values, one at the sender and one at the receiver. In contrast, the present invention does not calculate a hash value for the previously received encrypted content.

Therefore, the use of hash values in Yoshiura et al. and Johnson et al. is not the same as "**receiving a hash value...comparing the hash value received with a previously stored hash value** corresponding to the previously received encrypted digital content; **updating the usage conditions ... in response to the hash value received matching the previously stored hash value; and permitting at least one additional use ... without the need to re-receive the received encrypted digital content ...**" as recited in amended claim 1 of the instant application. Quite clearly, Yoshiura et al. and Johnson et al. use hash values to ***verify*** that a file has not changed during transmission, while the present invention uses hash values to ***identify*** a particular file that is already stored, to the exclusion of others.

Continuing further, the systems in Yoshiura and Johnson of digital signatures using hash values requires that the content be sent as part of the message in order to

---

[1] Applicants make no statement whether such combination is even proper.

[2] See www.whatis.com "*In addition to faster data retrieval, hashing is also used to encrypt and decrypt digital signatures (used to authenticate message senders and receivers). The digital signature is transformed with the hash function and then both the hashed value (known as a message-digest) and the signature are sent in separate transmissions to the receiver. Using the same hash function as the sender, the receiver derives a message-digest from the signature and compares it with the message-digest*

correctly calculate the hash value at the receiver. The Applicants submit that the combination of Yoshiura taken alone and/or in view of Johnson *teaches away* from "and without the need to re-receive the encrypted digital content being copied". Prior art that *teaches away* is per se demonstration of lack of *prima facie* obviousness.[3] Yoshiura and Johnson specifically *teach* using hashing with digital signatures where the digital signature (i.e. content) is hashed at both the sender and at the receiver. In the present invention, the receiver uses a previously stored hash value which is provided by the sender and compares it to a newly received hash value that has also been provided by the sender. A hash value is **never** calculated at the receiver with the present invention because there is no need to calculate a hash value for the previously received encrypted content. Accordingly, independent claims 1, 7, 9, 15, and18 distinguish over Yoshiura taken alone and/or in view Johnson of for at least this reason as well.

Independent claims 7, 9, 15, and 18 recite similar limitations as independent claim 1. Specifically, Stefik taken alone and/or in view of Yoshiura et al. and/or in view of Johnson et al. are completely silent on:

- Claim 7

  receiving from the electronic store **a second hash value**; and **determining if the first hash value received is identical to the second hash value** and in response to the first hash and the second hash value being identical, then authorizing the creating additional copies

- Claim 9

  receiving from an electronic store, a hash value, which uniquely identifies the encrypted digital content, associated with the request to acquire the encrypted digital content;

  comparing the hash value received from the electronic store with a previously stored hash value corresponding to the previously received encrypted digital content;

  updating the usage conditions associated with the previously received encrypted digital content **in response to the hash value received matching the previously stored hash value**; and

---

it also received. They should be the same."
[3] See In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)

permitting at least one additional use of the previously received encrypted digital content **without the need to re-receive the received encrypted digital content.**

- Claim 15

receiving a second hash value; and
determining if the first hash value received is identical to the second hash value and in response to the first hash and the second hash value being identical, then authorizing the creating additional copies

- Claim 18

means for receiving a hash value associated with the request to acquire the encrypted digital content;
means for **comparing the hash value received with a previously stored hash value** corresponding to the previously received encrypted digital content

Accordingly, independent claims 7, 9, 15, and 18 distinguish over Stefik taken alone and/or in view of Yoshiura et al. and/or in view of Johnson et al. for at least this reason.

For the foregoing reasons, independent claims 1, 7, 9, 15, and 18 distinguish over Stefik taken alone and/or in view of Yoshiura et al. and/or in view of Johnson et al. Claims 3-6, 8, 11-14, 16, 19-20 and 22 depend from independent claims 1, 7, 9, 15, and 18 respectively, and since dependent claims contain all the limitations of the independent claims, claims 3-6, 8, 11-14, 16, 19-20, and 22 distinguish over Stefik taken alone and/or in view of Yoshiura et al. and/or in view of Johnson et al., as well, and the Examiner's rejection should be withdrawn.

CONCLUSION

The remaining cited references have been reviewed and are not believed to effect the patentability of the claims as amended.

In this Response, Applicants have amended certain claims. In light of the Office Action, Applicants believe these amendments serve a useful clarification purpose, and are desirable for clarification purposes, independent of patentability. Accordingly,

Applicants respectfully submit that the claim amendments do not limit the range of any permissible equivalents.

Applicants acknowledge the continuing duty of candor and good faith to disclosure of information known to be material to the examination of this application. In accordance with 37 CFR § 1.56, all such information is dutifully made of record. The foreseeable equivalents of any territory surrendered by amendment is limited to the territory taught by the information of record. No other territory afforded by the doctrine of equivalents is knowingly surrendered and everything else is unforeseeable at the time of this amendment by the Applicants and their attorneys.

Applicants respectfully submit that all of the grounds for rejection stated in the Examiner's Office Action have been overcome, and that all claims in the application are allowable. No new matter has been added. It is believed that the application is now in condition for allowance, which allowance is respectfully requested.

PLEASE CALL the undersigned if that would expedite the prosecution of this application.

Respectfully submitted,

Date: April 8, 2005

By: _____
Scott Smiley, Reg. No. 55,827
Attorney for Applicants

By: _____
Jon Gibbons, Reg. No. 37,333
Attorney for Applicants

FLEIT, KAIN, GIBBONS, GUTMAN BONGINI & BIANCO P.L.
551 N.W. 77th Street, Suite 111
Boca Raton, FL 33487
Tel (561) 989-9811
Fax (561) 989-9812

Please Direct All Future Correspondence to Customer Number **23334**